The Federal Plan for Cyber Security and Information Assurance Research and Development

2006 NSTAC Research and Development Exchange Workshop

September 21, 2006

Simon Szykman, Ph.D.
Director
National Coordination Office for Networking and Information Technology Research and Development

Annabelle Lee
Director, Security Standards, Best Practices and R&D Requirements
Department of Homeland Security

Overview of the NITRD Program

- **Legislative bases for the Networking and Information Technology Research and Development (NITRD) Program**
  - High-Performance Computing Act of 1991
  - Next Generation Internet Research Act of 1998
- **NITRD Subcommittee, National Science and Technology Council (NSTC)**
  - Representatives from 14 program agencies + OMB + OSTP + NCO/NITRD
  - Has two Interagency Working Groups (IWGs) and five Coordinating Groups (CGs)
- **Budget of $3.1 billion proposed for FY 2007**

Agency NITRD Budgets by PCA

FY 2007 Budget Requests (dollars in millions)

Agency		High End Computing Infrastructure & Applications (HEC I&A)	High End Computing Research & Development (HEC R&D)	Cyber Security & Information Assurance (CSIA)	Human-Computer Interaction & Information Management (HCI &IM)	Large Scale Networking (LSN)	High Confidence Software & Systems (HCSS)	Social, Economic, & Workforce Implications of IT (SEW)	Software Design & Productivity (SDP)	Total
NSF	2006 Estimate	220.3	62.7	57.6	207.4	82.2	41.3	91.1	47.9	810.3
	2007 Request	**272.4**	**64.1**	**67.6**	**220.9**	**84.0**	**51.3**	**92.9**	**50.7**	**903.7**
OSD & DoD Service research orgs.		214.6	9.8	0.6	138.5	141.8	31.2	0.2	6.9	543.7
		186.0	**8.7**	**0.7**	**135.6**	**130.7**	**29.1**	**0.3**	**6.8**	**497.8**
NIH		198.5			188.7	74.9	8.4	12.3	17.9	500.6
		194.7			**183.2**	**74.6**	**8.3**	**12.2**	**17.7**	**490.7**
DARPA			94.1	78.7	174.2	21.3				368.3
			117.7	**81.6**	**233.2**	**33.2**				**465.7**
DOE/SC		104.4	109.1			38.9		3.5		255.8
		135.3	**160.4**			**45.0**		**4.0**		**344.7**
NSA			89.2	14.1		1.0	36.2			140.5
			62.4	**13.3**		**2.3**	**39.9**			**117.9**
NASA		60.3		1.3	2.0	5.7	7.0		1.8	78.1
		63.9		**1.3**	**2.0**	**6.0**	**7.0**		**1.8**	**82.0**
AHRQ					40.1	21.6				61.7
					37.3	**20.0**				**57.3**
NIST		2.3	1.2	9.1	7.8	4.3	9.6		4.6	38.9
		2.3	**1.2**	**11.1**	**9.8**	**4.3**	**9.6**		**4.6**	**42.9**
DOE/NNSA		10.0	15.9			1.6		4.6	3.3	35.4
		9.5	**23.4**			**1.6**		**4.6**	**2.8**	**41.9**
NOAA		11.4	1.9		0.2	0.7			1.6	15.8
		16.4	**1.9**		**0.5**	**2.9**			**1.6**	**23.3**
EPA		3.3			3.0					6.3
		3.3			**3.0**					**6.3**
TOTAL (2006 Estimate)		825.0	383.9	161.3	761.9	393.9	133.6	111.6	84.0	2,855
TOTAL (2007 Request)		**883.8**	**439.9**	**175.5**	**825.4**	**404.5**	**145.2**	**114.0**	**85.9**	**3,074**

NITRD National Coordination Office

- **Objectives:**
  - Support NITRD-related policy making in the White House Office of Science and Technology Policy (OSTP)
  - Serve as the Federal focal point for interagency technical planning, budget planning, and coordination for the Federal NITRD Program
  - Serve as a source of timely, high-quality, technically accurate, in-depth information on accomplishments, new directions, and critical challenges for the NITRD Program

NITRD Program Coordination Groups

White House
Executive Office of the President

Office of Science and Technology Policy

President's Council of Advisors on Science and Technology (PCAST) serving as the **President's Information Technology Advisory Committee (PITAC)**

National Science and Technology Council

Committee on Technology

Committee on Homeland and National Security

National Coordination Office (NCO) for Networking and Information Technology Research and Development

Subcommittee on Networking and Information Technology Research and Development (NITRD)

Subcommittee on Infrastructure

High End Computing (HEC) Interagency Working Group (HEC I&A and HEC R&D)

Cyber Security and Information Assurance (CSIA) Interagency Working Group

Human Computer Interaction and Information Management (HCI&IM) Coordinating Group

Large Scale Networking (LSN) Coordinating Group

High Confidence Software and Systems (HCSS) Coordinating Group

Social, Economic, and Workforce Implications of IT and IT Workforce Development (SEW) Coordinating Group

Software Design and Productivity (SDP) Coordinating Group

CSIA Program Component Area

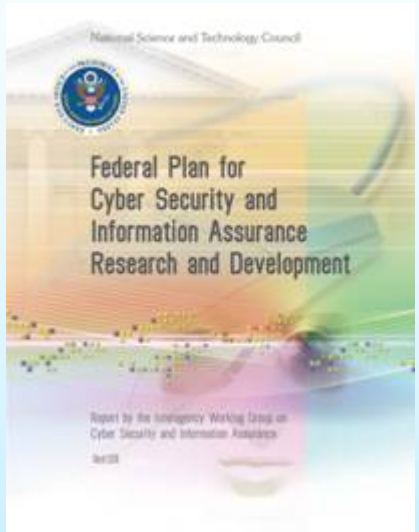
- **Cyber Security and Information Assurance (CSIA)**
  - R&D to protect computer-based systems from actions that compromise or threaten to compromise the authentication, availability, integrity, or confidentiality of these systems and/or the information they contain.
  - Coordinated through the CSIA Interagency Working Group (IWG)

The CSIA IWG

- **NITRD member agencies: DARPA, DHS, NASA, NIH, NIST, NSA, NSF, and OSD and DoD Service research organizations**
- **Participating agencies: CIA, DOE (LLNL), DOJ, DOT, DTO, FAA, FBI, State, Treasury, and TSWG**
- **Operations**
  - Co-chaired by representatives from OSTP and a Federal agency (currently DHS)
  - Holds monthly meetings
  - Conducts annual all-day "special meeting" of agency presentations to support interagency budget and program planning
  - Organizes workshops
- **Developed the *Federal Plan for Cyber Security and Information Assurance Research and Development***

Federal Plan for CSIA R&D

- **Federal Plan for CSIA R&D**
  - Plan development initiated in early 2004
  - Plan publicly released in April 2006
- **Scope is limited to unclassified R&D**
- **Objectives of the Federal Plan for CSIA R&D:**
  - To serve as a baseline for future roadmapping activities
  - To serve as the basis for future R&D policy, technical and investment decision making



Federal Plan for CSIA R&D

- **Process:**
  - Identify strategic Federal R&D objectives in the context of CSIA R&D
  - Identify a broad set of areas within CSIA R&D
  - Identify interagency technical R&D priorities among areas
  - Identify interagency investment priorities among areas
  - Define scope, state of the art, and identify capability gaps for R&D areas
  - Make broad findings and recommendations

Federal Plan for CSIA R&D

- **Strategic Federal R&D objectives relating to CSIA R&D:**

  (Derived from a review of policy and legislative requirements, analyses of cyber security threats and infrastructure vulnerabilities, and agency mission requirements)

  1. Support research, development, testing, and evaluation of cyber security and information assurance technologies aimed at preventing, protecting against, detecting, responding to, and recovering from cyber attacks that may have large-scale consequences
  2. Address cyber security and information assurance R&D needs that are unique to critical infrastructures
  3. Develop and accelerate the deployment of new communication protocols that better assure the security of information transmitted over networks.

Federal Plan for CSIA R&D

- **Strategic Federal R&D objectives:**
  4. Support the establishment of experimental environments such as testbeds that allow government, academic, and industry researchers to conduct a broad range of cyber security and information assurance development and assessment activities
  5. Provide a foundation for the long-term goal of economically informed, risk-based cyber security and information assurance decision making
  6. Provide novel and next-generation secure IT concepts and architectures through long-term research
  7. Facilitate technology transition and diffusion of Federally funded R&D results into commercial products and services and private-sector use

Federal Plan for CSIA R&D

- **Technical areas: about 50 topics in the following categories:**
  - Functional Cyber Security
  - Securing the Infrastructure
  - Domain-Specific Security
  - Cyber Security Characterization and Assessment
  - Foundations for Cyber Security
  - Enabling Technologies for Cyber Security and Information Assurance R&D
  - Advanced and Next-Generation Systems and Architecture for Cyber Security
  - Social Dimensions of Cyber Security

Technical and Funding Priorities

CSIA RESEARCH AREAS R&D Categories and Technical Topics	TOP PRIORITIES Technical	 Funding
1.Functional Cyber Security		
1.1 Authentication, authorization, and trust management	✓	✓
1.2 Access control and privilege management	✓	✓
1.3 Attack protection, prevention, and preemption	✓	✓
1.4 Large-scale cyber situational awareness	✓	
1.5 Automated attack detection, warning, and response		✓
1.6 Insider threat detection and mitigation		
1.7 Detection of hidden information and covert information flows		
1.8 Recovery and reconstitution		
1.9 Forensics, traceback, and attribution		
2. Securing the Infrastructure		
2.1 Secure Domain Name System		
2.2 Secure routing protocols		
2.3 IPv6, IPsec, and other Internet protocols		
2.4 Secure process control systems	✓	
3. Domain-Specific Security		
3.1 Wireless security	✓	✓
3.2 Secure radio frequency identification		
3.3 Security of converged networks and heterogeneous traffic	✓	
3.4 Next-generation priority services		

Technical and Funding Priorities

CSIA RESEARCH AREAS R&D Categories and Technical Topics	TOP PRIORITIES Technical	 Funding
4. Cyber Security Characterization and Assessment		
4.1 Software quality assessment and fault characterization		✓
4.2 Detection of vulnerabilities and malicious code	✓	
4.3 Cyber security standards		
4.4 Cyber security metrics		
4.5 Software testing and assessment tools	✓	✓
4.6 Risk-based decision making for cyber security		
4.7 Critical infrastructure dependencies and interdependencies		
5. Foundations for Cyber Security		
5.1 Hardware and firmware security		
5.2 Secure operating systems		
5.3 Security-centric programming languages		
5.4 Security technology and policy management methods and policy specification languages		
5.5 Information provenance		
5.6 Information integrity		
5.7 Cryptography		✓
5.8 Multi-level security		
5.9 Secure software engineering		✓
5.10 Fault tolerant and resilient systems		
5.11 Integrated, enterprise-wide security monitoring and management		
5.12 Analytical techniques for security across the IT systems engineering life cycle		✓

Technical and Funding Priorities

CSIA RESEARCH AREAS R&D Categories and Technical Topics	TOP PRIORITIES Technical	 Funding
6. Enabling Technologies for Cyber Security and Information Assurance R&D		
6.1 Cyber security and information assurance R&D testbeds		✓
6.2 IT system modeling, simulation, and visualization	✓	
6.3 Internet modeling, simulation, and visualization		
6.4 Network mapping		
6.5 Red teaming		
7. Advanced and Next-Generation Systems and Architectures for Cyber Security		
7.1 Trusted computing base architectures		✓
7.2 Inherently secure, high-assurance, and provably secure systems and architectures	✓	
7.3 Composable and scalable secure systems	✓	
7.4 Autonomic systems		✓
7.5 Architectures for next-generation Internet infrastructure	✓	
7.6 Quantum cryptography		
8. Social Dimensions of Cyber Security		
8.1 Trust in the Internet		
8.2 Privacy and cyber security	✓	

Analysis of CSIA R&D Priorities

- **Top priorities are intended to be informative**
  - Can help guide future technical and budget decision making
  - All areas – not just the top priorities – are important. Should not be interpreted to suggest divestment from areas that are not on the top priority list.
- **Priorities are largely consistent with R&D areas identified as important by other groups**
  - President's Information Technology Advisory Committee (PITAC)
  - INFOSEC Research Council (IRC)
- **Detailed comparison available in the plan document**

Analysis of CSIA R&D Priorities

- **Possible interpretations of differences between technical and funding priorities:**
  - Interagency technical priorities are not identical to agency priorities
    - It is expected that agencies focus on (and therefore fund) agency and mission priorities
  - Technical priorities evolve with time
    - Budget cycle creates time lag between identification of new priorities and flow of funding into those areas
  - Some technical areas may not be recognized as being as important as they are
  - Some technical areas may be recognized as important but may not be adequately addressed due to mismatches in actual or perceived mission scope
- **Interagency coordination needed to identify reasons for differences, and appropriate follow-on response.**

Findings and Recommendations

Findings and Recommendations:

1. ***Target Federal R&D investments to strategic cyber security and information assurance needs***
   - Federal CSIA R&D managers should reassess the Nation's strategic and longer-term CSIA needs to ensure that Federal R&D addresses those needs and avoids areas in which the private sector is productively engaged.
2. ***Focus on threats with the greatest potential impact***
   - Federal agencies should focus CSIA R&D investments on high-impact threats as well as on investigation of innovative approaches to increasing the overall security and information assurance of IT systems.

Findings and Recommendations

Findings and Recommendations:

3. ***Make cyber security and information assurance R&D both an individual agency and an interagency budget priority***
   - Agencies should consider CSIA R&D policy guidance as they address their mission-related R&D requirements. To achieve the greatest possible benefit from investments throughout the Federal government, CSIA R&D should have high priority for individual agencies as well as for coordinated interagency efforts.
4. ***Support sustained interagency coordination and collaboration on cyber security and information assurance R&D***
   - Sustained coordination and collaboration among agencies will be required to accomplish the goals identified in this Plan. The CSIA IWG should continue to be the primary vehicle for this R&D coordination and collaboration.

Findings and Recommendations

Findings and Recommendations:

5. ***Build security in from the beginning***
   - The Federal CSIA R&D portfolio should support fundamental R&D exploring inherently more secure next-generation technologies that will replace today's patching of the current insecure infrastructure.
6. ***Assess security implications of emerging information technologies***
   - The Federal government should assess the security implications and the potential impact of R&D results in new information technologies as they emerge in such fields as optical computing, quantum computing, and pervasively embedded computing.

Findings and Recommendations

Findings and Recommendations:

7. ***Develop a roadmap for Federal CSIA R&D***
   - Agencies should use this Plan's technical priorities and investment analyses to work with the private sector to develop a roadmap of CSIA R&D priorities. This effort should emphasize coordinated agency activities that address technical and investment gaps and should accelerate development of strategic capabilities.
8. ***Develop and apply new metrics to assess cyber security and information assurance***
   - As part of roadmapping, Federal agencies should develop and implement a multiagency plan to support the R&D for a new generation of methods and technologies for cost-effectively measuring IT component, network, and system security.

Findings and Recommendations

Findings and Recommendations:

9. Institute more effective coordination with the private sector

- The Federal government should review private sector CSIA practices and countermeasures to help identify capability gaps in existing technologies, and should engage the private sector in efforts to better understand private-sector views on CSIA R&D priorities. Federal agencies supporting CSIA R&D should improve communication and coordination with operators of both Federal and private-sector critical infrastructures with shared interests. Information exchange and outreach activities that accelerate technology transition should be integral parts of Federal CSIA R&D activities.

Findings and Recommendations

Findings and Recommendations:

10. Strengthen R&D partnerships, including those with international partners

- The Federal government should foster a broad partnership of government, the IT industry, researchers, and private-sector users to develop, test, and deploy a more secure next-generation Internet. The Federal government should initiate this partnership by holding a national workshop to solicit views and guidance on CSIA R&D needs from stakeholders outside of the Federal research community. In addition, impediments to collaborative international R&D should be identified and addressed in order to facilitate joint activities that support the common interests of the United States and international partners.

Federal Government Coordination

- **Coordination between the Federal government and the private sector, and with international partners, is critical:**
  - Private sector owns 85% of the Nation's critical (information) infrastructure, and has significant responsibility in ensuring its security
  - The private sector and international partners have knowledge and expertise the Federal government can benefit from
  - Federal government CSIA R&D funding resources are limited
  - The U.S. government, international partners, and the private sector (domestic and international) have shared interests, but also differing interests. This creates opportunities for leveraging investments by having complementary CSIA R&D efforts.

Future Steps

- **NITRD NCO plans:**
  - Currently in early planning stages of organizing workshop(s) on CSIA R&D needs
    - To include participation from government, industry and academia
    - Validate work done to date by the CSIA IWG
    - Gather input on CSIA R&D from non-government research community
    - Establish framework or outline for CSIA R&D Roadmap
  - CSIA IWG to initiate roadmapping effort as follow-on to development of the Federal CSIA R&D Plan

Comments or Questions?

- More detailed information on the NITRD Program is available in *The FY 2007 Supplement to the President's Budget for the NITRD Program*

- To download a copy of the Budget Supplement or the *Federal Plan for Cyber Security and Information Assurance R&D*, please visit:

  http://www.nitrd.gov